AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 1017

OFFERED BY MRS. WALORSKI OF INDIANA

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Veterans Information Security Improvement Act".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

SEC. 2. GOVERNANCE OF INFORMATION SECURITY PROGRAM OF DEPARTMENT OF VETERANS AFFAIRS.

(a) REQUIREMENTS FOR CERTAIN OFFICIALS AND STAFF.—

(1) IN GENERAL.—Subchapter III of chapter 57 of title 38, United States Code, is amended by inserting after section 5723 the following new section:

"§ 5723A. Governance of information security program

"(a) IN GENERAL.—The Secretary shall improve the transparency and the coordination of the information security program of the Department in accordance with this section.

"(b) OFFICE OF INFORMATION AND TECHNOLOGY.—(1) The Secretary shall ensure that the Assistant Secretary for Information and Technology, as the Chief Information Officer of the Department, possesses—

"(A) the appropriate education, validated experience, and capabilities in the management of information technology organizations;

"(B) an industry recognized certification in information security and cyber security defense; and

"(C) demonstrated, sound technical and business capabilities.

"(2) The Secretary shall ensure that the staff of the Office of Information and Technology who perform security functions, including the assessment and analysis of risk, security auditing, security operations, and security engineering, are assigned to the Office of Information Security.

"(3) The Secretary shall ensure that the Office of Information and Technology, in coordination with the head of the Office of Information Security, maintains appropriate information security functions, as applicable, to—

"(A) incorporate secure software assurance processes into the software development lifecycle for all software development activities;

"(B) validate that each third-party developed software used in any information system of the Department meets the standards of the National Institute of Standards and Technology with respect to security, safety, reliability, functionality and extensibility;

"(C) maintain established information security baseline controls for such information systems, and immediately remediate systems determined to be out of compliance with established baseline controls to the maximum extent possible;

"(D) ensure that the security architecture of the Department is documented and fully integrated into the overall enterprise architecture strategy of the Department;

"(E) ensure that the information system security plan or related documents of the Department addressing information security are detailed and fully integrated into the overall enterprise architecture strategy of the Department;

"(F) deploy and maintain centralized security monitoring capabilities capable of detecting and alerting of security events in real time;

"(G) design and deploy an effective incident response capability, including retention of industry experts in forensics, threat intelligence, and malware analysis;

"(H) develop and implement a policy that restricts the development of new data warehouses and data marts holding sensitive personal information of veterans and reduces the number of data marts holding such information;

"(I) protect sensitive information of the Department and sensitive personal information to a defined data classification policy in accordance with governance and compliance requirements, leveraging digital signature (authenticity and integrity) and digital rights management (confidentiality, authorization and audit) technology where appropriate; and

"(J) develop working relationships with other departments and agencies of the Federal Government whose information security efforts intersect in any way with the Department.

"(c) OFFICE OF INFORMATION SECURITY.—(1) The Secretary shall ensure that the head of the Office of Information Security possesses—

"(A) the appropriate education and validated experience with respect to information security;

"(B) an industry recognized certification in cyber security defense;

"(C) demonstrated, sound technical and business capabilities; and

"(D) other relevant experience.

"(2) The Secretary shall ensure that all of the field staff of the Office of Information Security, including relevant staff of the Office of Information Technology, whose primary responsibility is the protection of personally identifiable information of veterans maintain current information security training and possess a certain level of information security, cyber security defense, and technical capabilities and certifications as appropriate.".

(2) CLERICAL AMENDMENT.—The table of sections at the beginning of such chapter is amended

by inserting after the item relating to section 5723 the following new item:

"5723A. Governance of information security program.".

(b) DEFINITIONS.—Section 5721 of title 38, United States Code, is amended by adding at the end the following new paragraphs:

"(24) DATA MART.—The term 'data mart' means a subset of a data warehouse that contains information for a specific department or entity of an organization rather than the entire organization.

"(25) DATA WAREHOUSE.—The term 'data warehouse' means a collection of data designed to support management decision making that contains a wide variety of data that present a coherent picture of business conditions for an entire organization at a single point in time and whose development includes the development of systems to extract data from operating systems plus installation of a warehouse database system that provides managers flexible access to the data.

"(26) DIGITAL SIGNATURES.—The term 'digital signatures' means a special class of electronic signatures that use digital certificates and cryptographic algorithms to provide the recipients of electronic documents the ability to verify that the content—

"(A) has not been altered or tampered with; and

"(B) originated from the individual or entity that sent the document.

"(27) DIGITAL RIGHTS MANAGEMENT.—The term 'digital rights management' means providing owners of electronic documents the ability to dynamically control the use of that content, including, at a minimum, the ability to—

"(A) determine who is able to open and read the document;

"(B) determine what permissions to act upon the document are given to a recipient who opens the document; and

"(C) know what the recipient has done with the document.

"(28) MALWARE.—The term 'malware' means malicious software used to perform unwanted actions on a computer, a network, or computing environment.".

SEC. 3. SECURITY OF CRITICAL NETWORK INFRASTRUCTURE, INCLUDING DOMAIN CONTROLLER, OF DEPARTMENT OF VETERANS AFFAIRS.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Veterans Affairs shall ensure the security and safeguard of the network infrastructure of the Department of Veterans Affairs.

(b) ACTIONS REQUIRED.—In carrying out subsection (a), the Secretary shall carry out the following actions:

(1) Maintain the awareness and complete physical and logical control of the critical network infrastructure, including routers, switches, domain naming systems, firewalls, load balancers, proxy devices, authentication services, telecommunications, domain controllers, and any device that is part of the trusted Internet connection system.

(2) Provide special security configurations for protecting critical infrastructure devices and services.

(3) Implement policies and security measures that minimize the threats to critical infrastructure devices and services.

(4) Ensure that critical infrastructure devices and services, including the domain controller settings, are in compliance with the Server Security Plan of the Department under the Department of Veterans Affairs Handbook 6500.

(5) Establish access rights, permissions, and multifactor authentication for the critical infrastruc-

ture devices and services, including the domain controller, for specific users or groups of users.

(6) Ensure that proper physical security measures are taken to safeguard the critical infrastructure devices and services and limit physical access to such location to a limited number of authorized individuals.

(7) Limit the access from network connections to critical infrastructure devices and services and only configure services and software that are needed by the devices and services.

(8) Disable or delete any service or software from critical infrastructure devices and services that is unnecessary.

(9) Where feasible, secure critical infrastructure devices and services with host-based and network-based security controls and limit the number of ports that are opened between critical infrastructure devices and services, including any device requesting access to network resources and services.

(10) Ensure that for any device to access and communicate with critical infrastructure devices and services within the domain, the authentication traffic has to be signed and encrypted.

(11) Limit the administrator account from accessing critical infrastructure devices and services, including domain controllers, throughout the network and use such account only for emergencies.

(12) Restrict remote access to local administrator accounts and use firewall rules to restrict lateral movement on the network.

(13) Ensure that information leaving a network is properly encrypted by employing enterprise-wide content-centric security or digital rights management to encrypt, analyze, and monitor sensitive information after such information leave a content management system.

(c) DETECTION ACTIONS REQUIRED.—In carrying out subsection (a), the Secretary shall carry out the following actions to detect a network intrusion:

(1) Demonstrate the applicability of the risk management framework as identified by the National Institute of Standards and Technology in the selection, implementation, assessment, and ongoing monitoring of privacy controls deployed in information systems, programs, and organizations of the Federal Government.

(2) Ensure that network- and host-based intrusion detection systems are deployed and properly

configured on high-risk systems and areas of the network.

(3) Ensure that proper auditing and event logging are configured into servers, user systems, firewalls, networking devices, applications, and domain controllers.

(4) Ensure that audit and event logs are forwarded and collected in a central repository for storage and analysis.

(5) Conduct regular audits and testing of the backups and restore events of the critical infrastructure devices and services.

(6) Conduct regular formal penetration testing to test for potential security weaknesses and resolve such weaknesses by not later than seven days after identifying such weaknesses.

(7) Deploy proper log review capabilities, including automated and manual methods, including through a security information and event monitoring solution, that are able to detect, at a minimum—

(A) events tied to known signatures, including common malware and exploits;

(B) network traffic attempting to access known malicious Internet Protocol addresses, uniform resource locators, or domains;

(C) changes in network traffic behavior, including unexpected traffic over abnormal ports;

(D) application level events, including attempted injection attacks;

(E) abnormal use of user, application, or privileged accounts; and

(F) attempted or successful movement of sensitive data in any unapproved, unencrypted manner.

(d) ACTIONS BASED ON DETECTION REQUIRED.—In carrying out subsection (a), if a network intrusion is detected, the Secretary shall carry out the following actions:

(1) Ensure that events identified through the security monitoring process are properly investigated and resolved through a defined incident response process staffed by trained responders supplemented by external industry experts retained as necessary with capabilities, including capabilities regarding—

(A) analysis of events generated by monitoring solutions;

(B) pre-planned responses to common attack types, including defacement, denial of service, malware outbreaks, and advanced persistent threat level threats;

(C) reverse engineering of attack methods, exploits, and malware;

(D) understanding of common hacking techniques, including initial infiltration, expansion, persistence, exfiltration, and the forensic and analysis methods to detect each such technique; and

(E) planned and exercised methods to address the priority of addressing threats and responding to such prioritized threats, including with respect to the isolation of individual systems or entire network segments, mass password resets, and deployment of emergency firewall or network changes meant to limit Internet connectivity to only critical services.

(2) If the Secretary determines that any critical network infrastructure device or service has been compromised, restore the device or service to the last known noncompromised state and determine the cause of the compromise.

(3) If the Secretary determines that compromised devices or services must be used for a limited time, conduct such use in accordance with the guidance established by the National Security Agency under the document titled ‘‘Information Assur-

ance Guidance for Operating on a Compromised Network'', or successor document.

(e) CERTIFICATION.—Not later than 30 days after the date of the enactment of this Act, the Secretary shall submit to the congressional veterans committees written certification that the Secretary has commenced each action described in subsections (b), (c), and (d).

SEC. 4. SECURITY OF COMPUTERS AND SERVERS OF DEPARTMENT OF VETERANS AFFAIRS.

(a) IN GENERAL.—The Secretary shall ensure the security of each general purpose computer and server of the Department.

(b) ACTIONS REQUIRED.—In carrying out subsection (a), the Secretary shall carry out the following actions:

(1) Formalize and enforce a Department-wide process to monitor software installed on general purpose computers and servers of the Department, prevent the unauthorized installation of software, and remove any unauthorized software that has been installed.

(2) Not later than 45 days after the date of the enactment of this Act, implement automated patching tools and processes that ensure that security patches are installed for any software or oper-

ating system on a computer by not later than 48 hours after the patch is made available.

(3) Employ automated tools to continuously monitor general purpose computers, servers, and mobile devices for active, up-to-date anti-malware protection with antivirus, antispyware, personal firewalls, and host-based intrusion prevention system functionality.

(4) Centralize oversight and control to effectively administer patch management processes (but the responsibility for testing and applying patches to specific systems may be decentralized to the component level).

(5) Perform regular scans of general purpose computers and servers to discover security vulnerabilities and log the results of such scans.

(6) Perform a patch-focused risk assessment to evaluate each system, database, and general purpose computer for threats, vulnerabilities, and its criticality to the mission of the Department.

(7) If the Secretary determines any security vulnerability—

(A) develop a test for the vulnerability and determine the cause of the vulnerability;

(B) address the vulnerability, including by patching, implementing a compensating control, or documenting and accepting a reasonable business risk (in accordance with industry accepted best practices) with respect to the vulnerability; and

(C) perform a post remediation scan to verify that the vulnerability was so addressed.

(8) Establish and ensure the use of standard, secure configurations of each operating system in use on the computers of the Department.

(9) Employ system-scanning tools that check computers daily for software version, patch levels, and configuration files.

(10) Deploy a security content automation protocol tool that is validated by the National Institute of Standards and Technology to use specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation.

(11) Standardize policies, procedures, and tools for effective patch management, including by assigning roles and responsibilities, performing risk assessments, and testing patches.

(12) Test each patch against all system configurations of the Department in a test environment

to determine any effect on the network before deploying the patch to the affected systems and monitor the status of the patches after deployment.

(13) Establish and maintain an inventory of all hardware equipment, software packages, services, and other technologies installed and used by the Department for patch management.

(14) Establish a policy for security fixes that is clearly communicated to computer users to ensure that the users are aware of—

(A) the versions of software or operating systems that are supported with respect to security fixes; and

(B) when software, operating systems, or other products are scheduled to no longer be maintained.

(15) Ensure that—

(A) the staff or contractors of the Department who are involved in patch management have the skills and knowledge needed to perform the responsibilities relating to such management; and

(B) system administrators are trained in identifying new patches and vulnerabilities.

(c) CERTIFICATION.—Not later than 30 days after the date of the enactment of this Act, the Secretary shall submit to the congressional veterans committees written certification that the Secretary has commenced each action described in subsection (b).

SEC. 5. UPGRADE OR PHASE-OUT OF UNSUPPORTED OR OUTDATED OPERATING SYSTEMS.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary shall ensure that the Secretary upgrades or phases out outdated or unsupported operating systems to protect computers of the Department from harmful viruses, spyware, and other malicious software that could affect the confidentiality of sensitive personal information of veterans.

(b) ACTIONS REQUIRED.—In carrying out subsection (a), the Secretary shall carry out the following activities:

(1) Establish a plan for phasing out outdated or unsupported operating systems used by the Department.

(2) Establish a policy to ensure that outdated and unsupported operating systems used by the Department do not connect to the network of the Department by not later than 15 days after the date on which such operating systems are so outdated or

unsupported, as determined appropriate by the Secretary.

(3) Establish a configuration management process to ensure that—

(A) a secure image that is regularly updated is used to build all new computers used by the Department; and

(B) any computer used by the Department that becomes compromised is re-imaged using such image.

(4) Implement applicable operating systems based on security guidance identified by the Information Assurance Directorate of the National Security Agency.

(5) Appropriately configure and test required software that was designed to be used on older operating systems to ensure the software is usable on a new operating system used by the Department.

(6) Limit administrative privileges to very few users who have both the appropriate knowledge and business need to modify the configuration of the operating system.

(7) Until the date on which an unsupported operating system is replaced, if a computer uses such operating system, disable web browser plug-ins, use

a hardware firewall, and if practicable, disconnect the computer from the network and do not use the computer to access the Internet.

(8) Deploy a software inventory tool to cover each of the operating systems in use by the Department to track—

(A) the type of such operating systems being used by the Department; and

(B) with respect to each computer of the Department—

(i) the type of operating system installed and the version number and patch level of such operating system; and

(ii) the software being used on such operating system.

(9) Regularly use file integrity checking tools to check any changes to critical operating systems, services, and configuration files.

(c) CERTIFICATION.—Not later than 30 days after the date of the enactment of this Act, the Secretary shall submit to the congressional veterans committees written certification that the Secretary has commenced each action described in subsection (b).

SEC. 6. SECURITY OF WEB APPLICATIONS FROM VITAL VULNERABILITIES.

(a) IN GENERAL.—The Secretary shall ensure that web applications used by the Department are secure from vulnerabilities that could affect the confidentiality of sensitive personal information of veterans.

(b) ACTIONS REQUIRED.—In carrying out subsection (a), the Secretary shall carry out the following activities:

(1) Not later than 60 days after the date of the enactment of this Act, develop a plan, including required actions and milestones, to fully remediate all security vulnerabilities described in subsection (a) that exist as of the date of the enactment of this Act.

(2) Develop detailed guidance for remediating each critical security vulnerability.

(3) Use best practices and lessons learned, including such practices and lessons described by the National Institute of Standards and Technology and the Open Web Application Security Project, to address the security vulnerabilities of web applications.

(4) Limit the permissions on the database logon used by web applications to only what is needed to reduce the effectiveness of any attack that exploits bugs in the application.

(5) Provide to web application developers—

(A) thorough application development guidance to ensure that new applications are designed by taking into account security; and

(B) detailed guidance on testing existing web applications for security vulnerabilities, including buffer overflows and cross-site scripting.

(6) Configure administrative passwords to be—

(A) complex and consist only of strings of letters, numbers, and characters that do not form a recognizable word; and

(B) changed every 90 days, in accordance with industry best practices.

(7) With respect to passwords used in connection with web applications, store the passwords for each system of the Department only in a well-hashed or encrypted format.

(8) Implement two-factor authentication technology requirements throughout the Department.

(9) If vulnerabilities in a web application are found, administer a full-source code review to determine if the vulnerabilities exist elsewhere within the code of the application.

(10) Periodically review user access to networks and web applications to identify unnecessary, inactive, or terminated user accounts.

(11) Establish a single set of strong authentication and session management controls that meet all the authentication and session management requirements defined in the Application Security Verification Standard of the Open Web Application Security Project.

(12) Implement visibility and attribution measures to improve the process, architecture, and technical capabilities of the Department to monitor web applications used on the networks and computers of the Department to detect attack attempts, locate points of entry, identify already compromised machines, interrupt activities of infiltrated attackers, and gain information about the sources of an attack.

(c) CERTIFICATION.—Not later than 30 days after the date of the enactment of this Act, the Secretary shall submit to the congressional veterans committees written certification that the Secretary has commenced each action described in subsection (b).

SEC. 7. SECURITY OF THE VISTA SYSTEM.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary shall ensure that the covered system is secure from vulnerabilities that could affect the confidentiality of sensitive personal information of veterans.

(b) Actions Required.—In carrying out subsection (a), the Secretary shall carry out the following activities:

(1) Develop a remedial action plan to address the approaches to interoperability—

(A) between multiple covered systems; and

(B) between the covered system and external systems and software.

(2) Update the policy, procedures, and governance of the Department with respect to system-to-system integration where users log on to external systems and then automatically connect to the covered system and interact.

(3) Provide authentication for the machine-to-machine broker so that the covered system ''listener'' verifies the identity of the calling system.

(4) Establish and implement policy with respect to the authentication of external systems attempting to connect to the covered system and criteria by which user authentication must be accomplished to ensure all applications that connect to the covered system convey accurate user information.

(5) Establish a business requirement that system-to-system integration connectivity across the wide-area network must consist of encrypted communication and require external systems to securely identify themselves, or for the covered system to securely identify external systems that attempt to connect to the system.

(6) Establish a business requirement that external systems communicate accurate user information to the covered system relating to actions initiated by actual individuals and facilitate the revocation of access by the covered system relative to specific users or external systems attempting to connect.

(7) Implement monthly project design reviews of the integration between systems and web applications to ensure that the effectiveness of the existing controls is sustained.

(8) Assess the potential compromise to non-Department networks that are interconnected with the network of the Department, including the networks of the Department of Defense and the Department of Health and Human Services.

(9) Ensure that, in the near-term, software development for the covered system develops the critical enhancements and fixes to the system that are

necessary to ensure compliance with changes to patient enrollment.

(10) Ensure that all systems of the Department have been given the ''Authority to Operate'' designation and have been properly certified by meeting all requirements, including a comprehensive assessment of management, operational, and technical security controls, to become operational, and restrict the use of waivers.

(c) CERTIFICATION.—Not later than 30 days after the date of the enactment of this Act, the Secretary shall submit to the congressional veterans committees written certification that the Secretary has commenced each action described in subsection (b).

(d) COVERED SYSTEM DEFINED.—In this section, the term ''covered system'' means the Veterans Health Information Systems and Technology Architecture of the Department of Veterans Affairs (commonly known as the ''VistA system'') that allows for an integrated inpatient and outpatient electronic health record for patients and provides administrative tools to employees of the Department.

SEC. 8. REPORT ON COMPLIANCE WITH INFORMATION SECURITY REQUIREMENTS AND BEST PRACTICES.

Not later than 60 days after the date of the enactment of this Act, the Secretary of Veterans Affairs shall submit to the congressional veterans committees the following:

(1) Written certification that the Secretary is taking every action required to comply with—

(A) subchapter III of chapter 57 of title 38, United States Code;

(B) subchapter III of chapter 35 of title 44, United States Code;

(C) special publications 800–53 and 800–111 of the National Institute of Standards and Technology, including with respect to encrypting databases;

(D) applicable memoranda issued by the Director of Management and Budget regarding protecting personally identifiable information and continuous monitoring; and

(E) any other relevant law or regulation regarding the information security of the Department of Veterans Affairs.

(2) How the Secretary is using and implementing the principles and best practices regarding

improving information security, including with respect to such principles and practices described in the document titled ''Framework for Improving Critical Infrastructure Cybersecurity'' of the National Institute of Standards and Technology.

SEC. 9. REPORTS ON IMPLEMENTATION.

(a) BIANNUAL REPORTS.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and every 180-day period thereafter, the Secretary shall submit to the congressional veterans committees a report on the implementation of this Act, including the amendments made by this Act.

(2) MATTERS INCLUDED.—Each report under subsection (a) shall include the following:

(A) A description of the actions taken by the Secretary to implement and comply with sections 2 through 7.

(B) A timeline and project plan, both short-term and long-term, for implementing each of sections 2 through 7 and assigning roles and responsibilities under such plan.

(C) Performance measures, defined metrics, and benchmarks to measure the results of the Secretary in carrying out remediation efforts under sections 2 through 7.

(D) A description of the best practices and lessons learned by the Secretary in carrying out sections 2 through 7.

(E) The progress made by the Secretary during each month covered by the report with respect to reducing the total number of outdated operating systems, web application vulnerabilities, critical security vulnerabilities, and other matters covered by sections 2 through 7.

(F) An appendix containing detailed reports of the Department, including the enterprise information technology dashboard and reports regarding security vulnerabilities, operating system trends, web applications, and progress made by the Secretary in addressing information security related recommendations made by the Comptroller General of the United States and the Inspector General of the Department of Veterans Affairs.

(b) ANNUAL INSPECTOR GENERAL REPORT.—The Inspector General of the Department of Veterans Affairs shall submit to the congressional veterans committees an annual report that includes a comprehensive assessment of the adequacy and effectiveness of the implementation by the Secretary of Veterans Affairs of sections 2 through 7, including the amendments made by this Act.

(c) MONTHLY REPORTS.—On a monthly basis, the Secretary shall submit to the congressional veterans committees reports on security vulnerabilities discovered pursuant to the actions taken under section 4(b)(5).

SEC. 10. APPLICATION.

In carrying out this Act, including the amendments made by this Act, the Secretary of Veterans Affairs may substitute a new risk-based technology or process relating to information security for a specific technology or process relating to information security described in this Act, including the amendments made by this Act, if the Secretary determines that such new technology or process—

(1) is a successor to the specific technology or process described in this Act, including the amendments made by this Act; and

(2) provides a greater amount of information security than would be provided if the Secretary did not make such substitution.

SEC. 11. DEFINITIONS.

In this Act:

(1) The term ‘‘Authority to Operate’’ means the official management decision given by a senior official of the Department to authorize operation of an information system and to explicitly accept the risk to the operations of the Department (including with respect to the mission, functions, image, or reputation of the Department), the assets and individuals of the Department, other elements of the Federal Government, and the United States based on the implementation of an agreed-upon set of security controls.

(2) The term ‘‘confidentiality’’ has the meaning given that term in section 5727 of title 38, United States Code.

(3) The term ‘‘congressional veterans committees’’ means the Committees on Veterans' Affairs of the House of Representatives and the Senate.

(4) The term ‘‘critical network infrastructure’’ means information technology hardware that provides—

(A) vital network services to the Department that is vital to carrying out the mission of the Department; and

(B) communications, security, transportation, access, and authentication services and capabilities.

(5) The term ‘‘domain controller’’ means a server that responds to security authentication requests responsible for allowing host access to domain resources by authenticating users, sorting user account information, and enforcing security policy.

(6) The term ‘‘general purpose computer’’ means a computer that, given the appropriate application and required time, should be able to perform most common computing tasks. Such term includes personal computers, including desktops, notebooks, smart phones, and tablets.

(7) The term ‘‘image’’ means a standard set of software (including the operating system and other software) that is installed on a computer.

(8) The term ‘‘information security’’ has the meaning given that term in section 5727 of title 38, United States Code.

(9) The term ‘‘information system’’ has the meaning given that term in section 5727 of title 38, United States Code.

(10) The term ‘‘malware’’ means malicious software used to perform unwanted actions on a computer, a network, or computing environment.

(11) The term ‘‘sensitive personal information’’ has the meaning given that term in section 5727 of title 38, United States Code.

(12) The term ‘‘web application’’ means an application in which all or some parts of the software are downloaded from the Internet each time the software is accessed, including web browser-based software that run within a web browser, desktop software that does not use a web browser, and mobile software that accesses the Internet for additional information.

(13) The term ‘‘well-hashed’’ means the process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.

☒